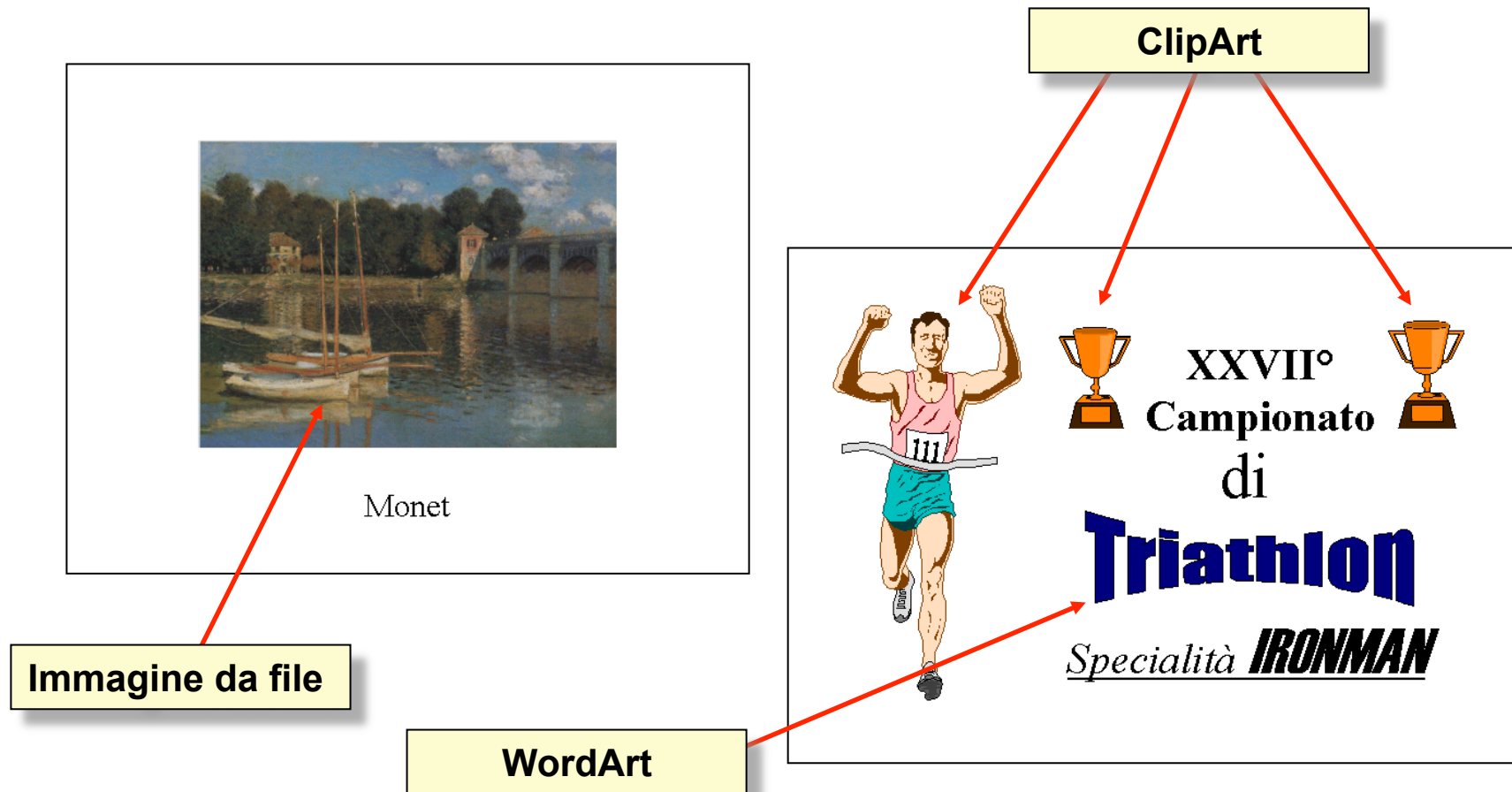


Esercitazioni di Microsoft Word/2

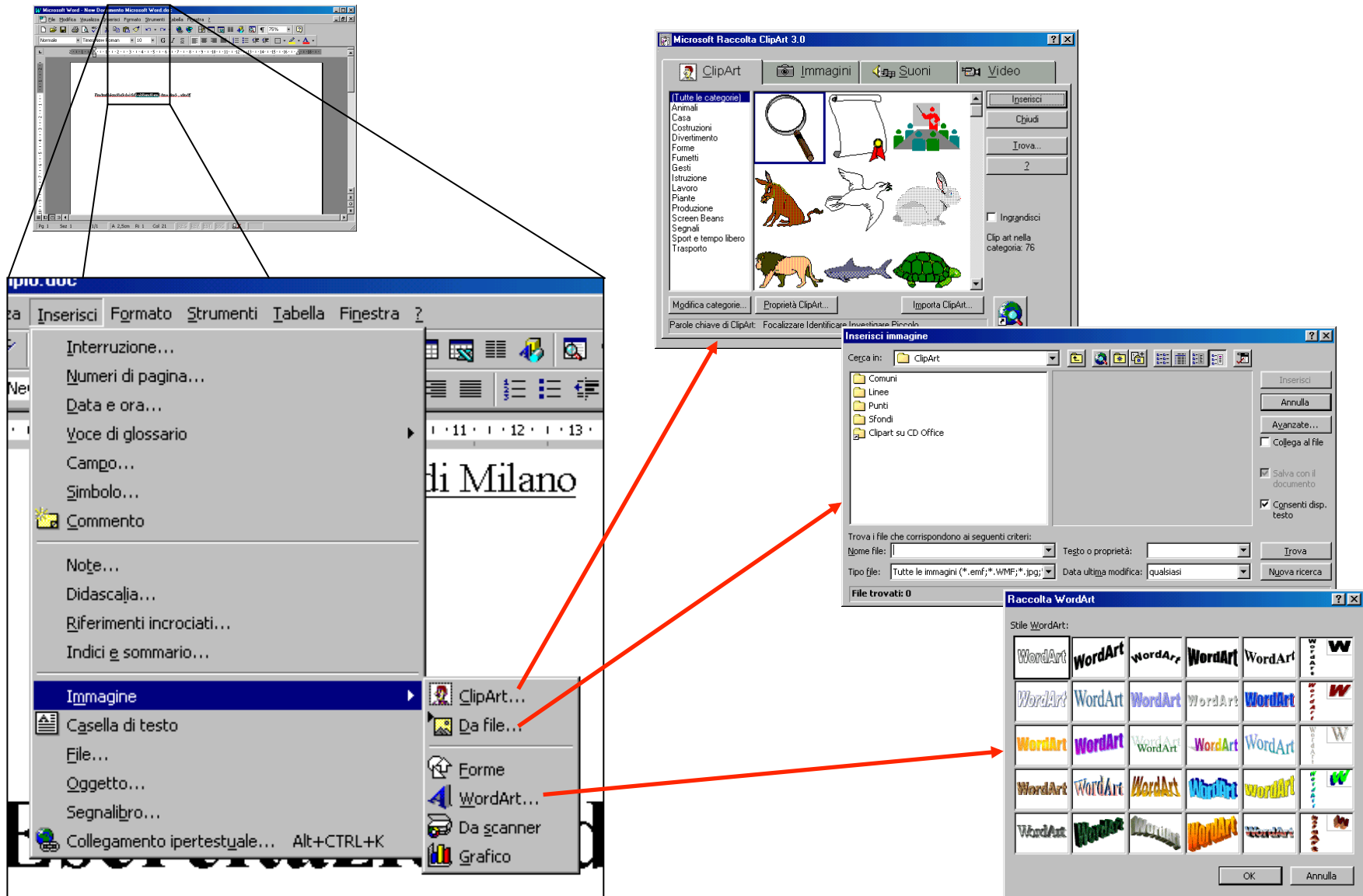
Alcune funzioni avanzate

Inserimento di immagini/1

- E' possibile inserire nel testo ClipArt, WordArt o immagini personalizzate.

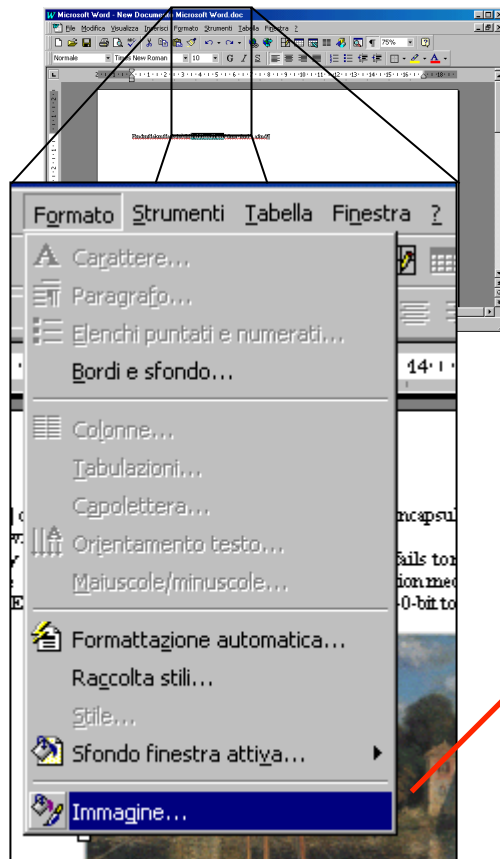


Inserimento di immagini/2

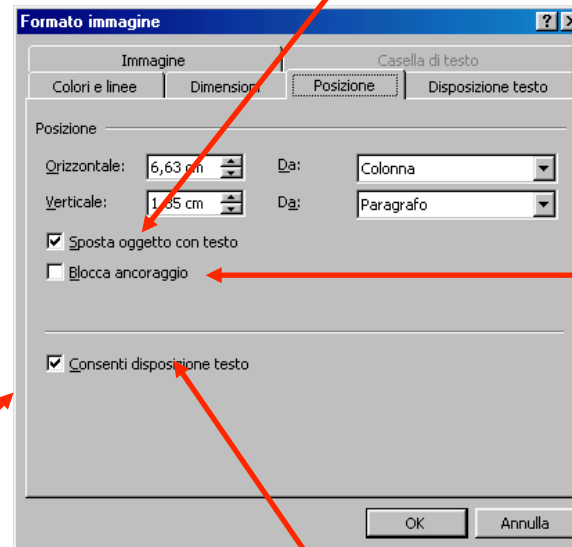


Inserimento di immagini/3

- Selezionando **Formato**→**Immagine...** è possibile definire la disposizione del testo rispetto all'immagine...



Adatta la posizione dell'immagine con il testo



Ancora la posizione dell'immagine alla pagina

Consenti la disposizione del testo

Inserimento di immagini/4


- ... La cartella **Disposizione Testo** definisce il modo con cui il testo è disposto intorno all'immagine

The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, as an encryption of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally considers that the WEP encryption fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3]) for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP "could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.

This report makes three design choices to share privacy with the WEP key size. The submission reports several attacks against WEP that succeed either in particular, or commonly, or in a fundamentally neutral encryption manner. WEP's range of encryption construction, its WEP resistance to key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's vulnerability prevents the WEP encryption from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encryption design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly suggests cryptographic parameters whose characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms.

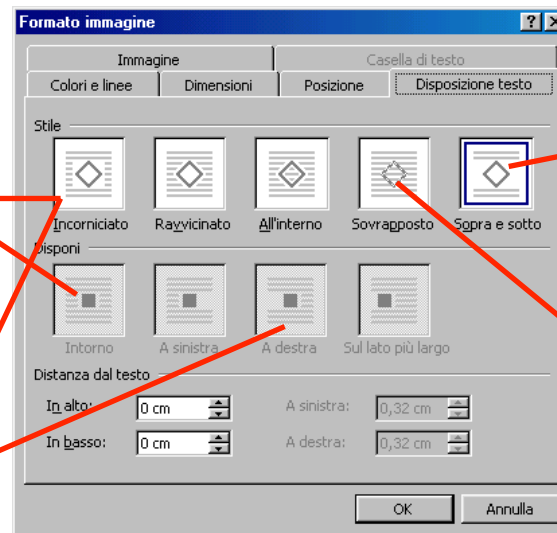



The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, as an encryption of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally considers that the WEP encryption fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3]) for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP "could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.

This report makes three design choices to share privacy with the WEP key size. The submission reports several attacks against WEP that succeed either in particular, or commonly, or in a fundamentally neutral encryption manner. WEP's range of encryption construction, its WEP resistance to key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's vulnerability prevents the WEP encryption from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encryption design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly suggests cryptographic parameters whose characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms and a replacement encryption.




The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, as an encryption of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally considers that the WEP encryption fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3]) for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP "could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.

This report makes three design choices to share privacy with the WEP encryption by simply increasing key size. The submission reports several attacks against WEP that succeed regardless of the key size or the cipher. In particular, as commonly defined, WEP's range of encryption is a fundamentally neutral construction, the WEP encryption remains secure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of a substitution cipher. This vulnerability prevents the WEP encryption from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encryption design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly suggests cryptographic parameters whose characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms and a replacement encryption.

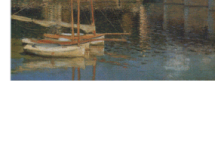


The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, as an encryption of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally considers that the WEP encryption fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3]) for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP "could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.

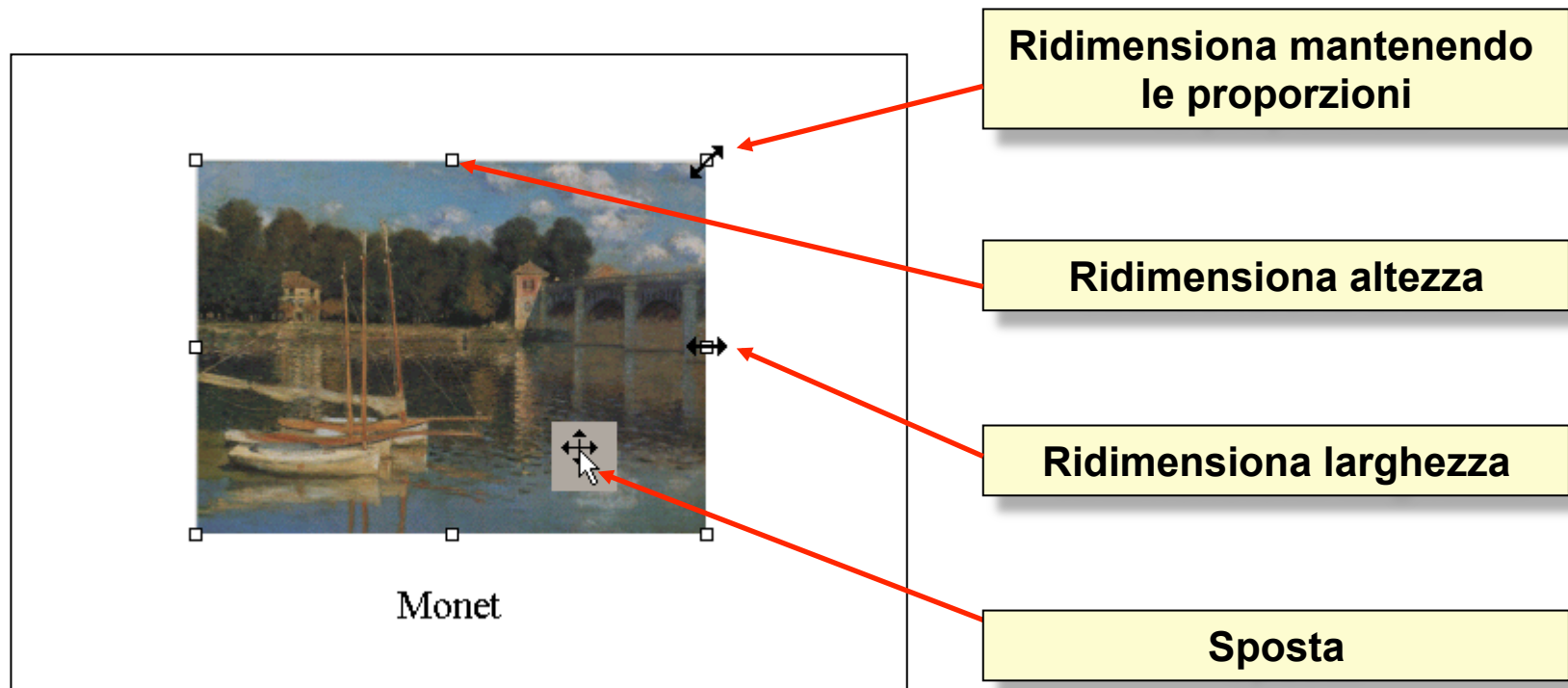
This report makes three design choices to share privacy with the WEP encryption by simply increasing key size. The submission reports several attacks against WEP that succeed regardless of the key size or the cipher. In particular, as commonly defined, WEP's range of encryption is a fundamentally neutral construction, the WEP encryption remains secure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of a substitution cipher. This vulnerability prevents the WEP encryption from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encryption design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly suggests cryptographic parameters whose characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms and a replacement encryption.



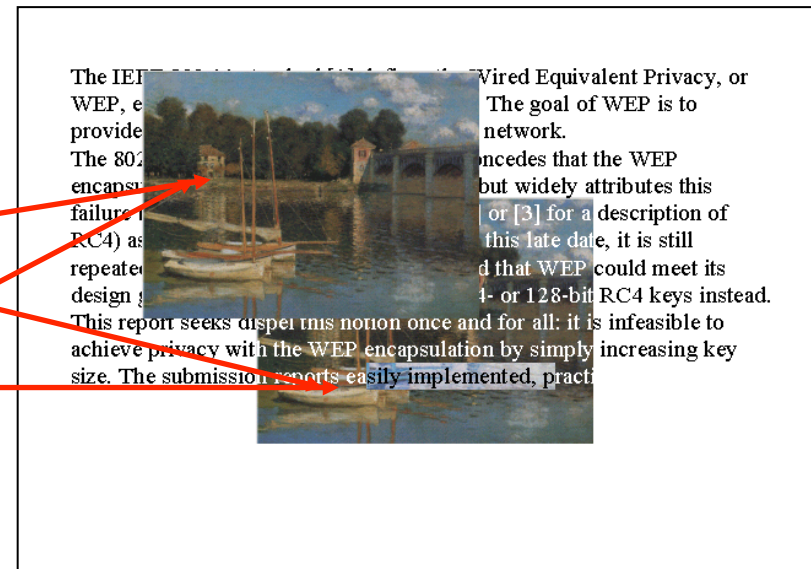
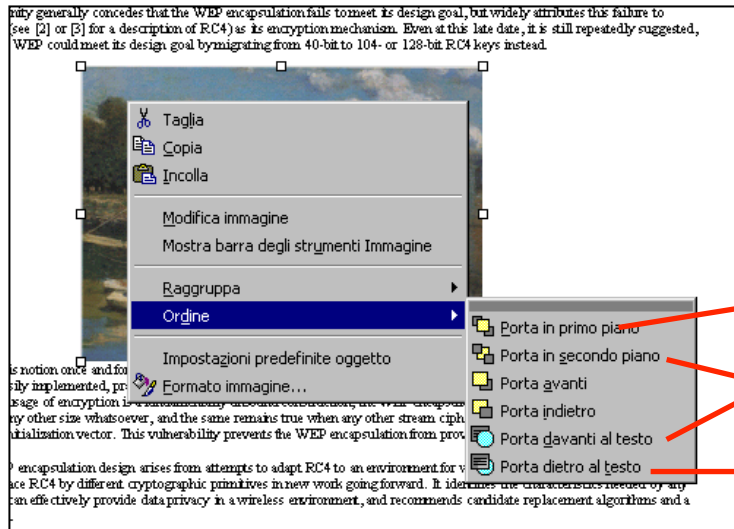
Inserimento di immagini/5

- Tenendo premuto il tasto sinistro del mouse è possibile spostare/ridimensionare le immagini inserite.

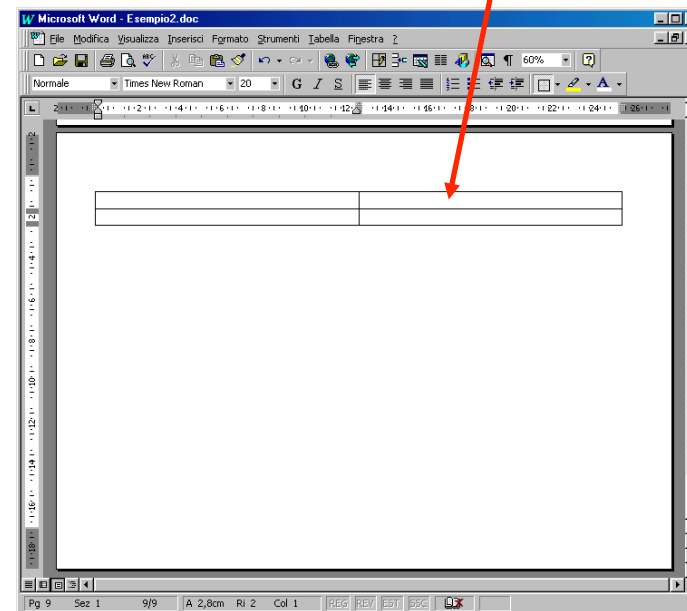
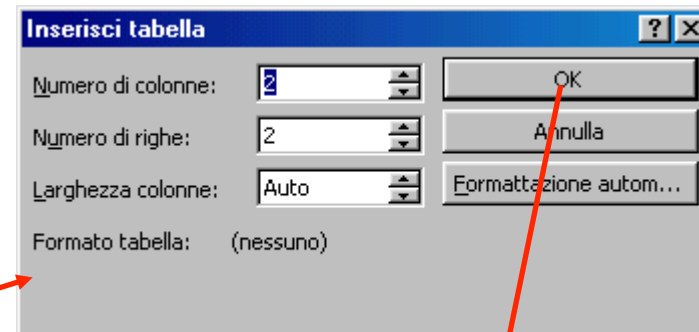
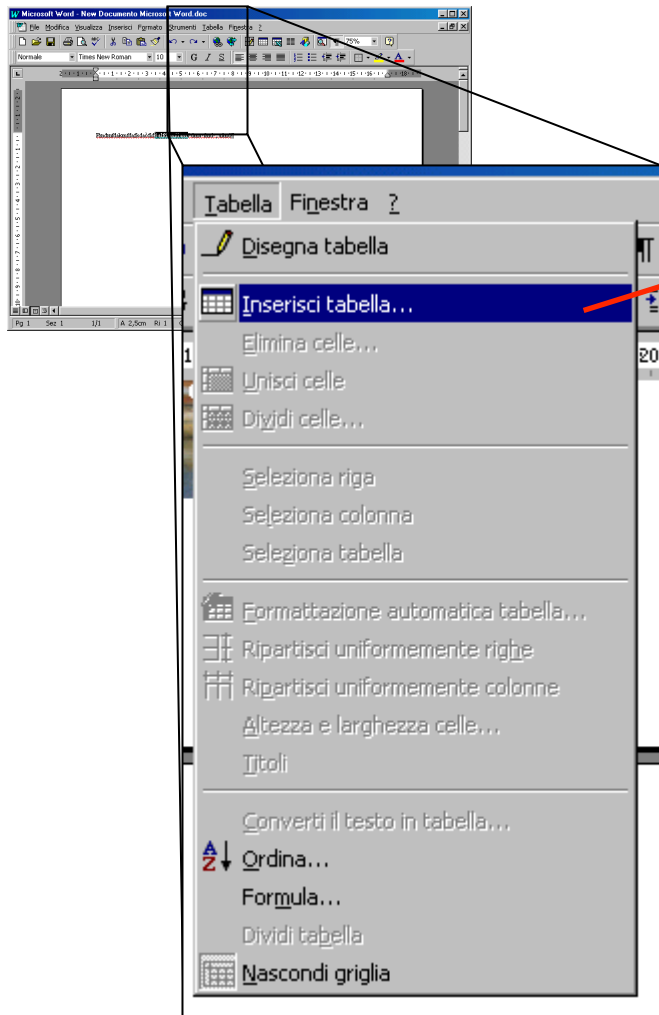


Inserimento di immagini/6

- Cliccando con il tasto destro sopra l'immagine e selezionando la voce **Ordine** si definisce la profondità delle figure.



Inserimento di tabelle/1



Inserimento di tabelle/2

The image shows a Microsoft Word window titled "Esempio2.doc" with a table containing five columns and three rows. Red arrows point from yellow callout boxes to specific parts of the table and the software interface:

- Larghezza colonne**: Points to the horizontal grid lines at the top of the table.
- Allineamento in verticale**: Points to text within the table cells, such as "Questa cella è allineata in alto", "Questa cella è allineata al centro", and "Questa cella è allineata in basso".
- Altezza righe**: Points to the vertical grid lines on the left side of the table.
- Orientamento in verticale**: Points to text rotated 90 degrees, such as "Questa cella è orientata in verticale".

A context menu is open in the bottom right corner, with an arrow pointing to the "Orientamento testo..." option. The menu includes options like "Taglia", "Copia", "Incolla", "Inserisci righe", "Elimina celle...", "Dividi celle...", "Disegna tabella", "Bordi e sfondo...", "Formattazione automatica tabella...", "Orientamento testo...", "Allineamento", and "Elenchi puntati e numerati...".

| | | | | |
|---------------------------------------|---------------------------------------|----------------------------------|------------------------------------|-----------------------------------|
| Questa è una cella | | | | |
| Questa cella è orientata in verticale | Questa cella è orientata in verticale | Questa cella è allineata in alto | Questa cella è allineata al centro | Questa cella è allineata in basso |
| | | | | |
| | | | | |

Inserimento di tabelle/3

- La funzionalità **Unisci/Dividi celle** permette di definire celle su più colonne/righe.

The diagram illustrates the 'Unisci/Dividi celle' functionality in a spreadsheet application. It shows a table with a merged cell and two split cells, with arrows pointing to the 'Unisci celle' and 'Dividi celle...' menu options.

Table Structure:

| | | | |
|---|---|--|--|
| | Questa cella è ottenuta unendo celle contigue sulla stessa riga | | |
| Questa cella è ottenuta unendo celle contigue sulla stessa riga | | | |
| | Queste celle sono ottenute dividendo una singola cella | Queste celle sono ottenute dividendo una singola cella | |

Menu Options:

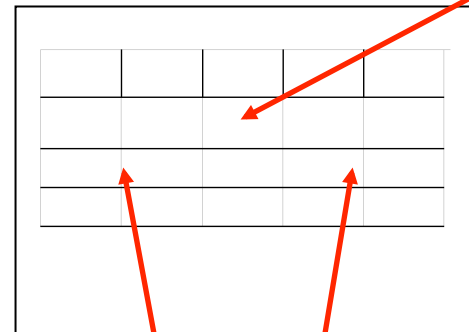
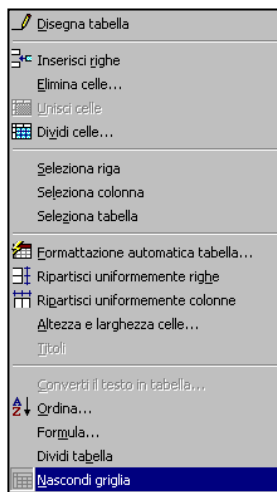
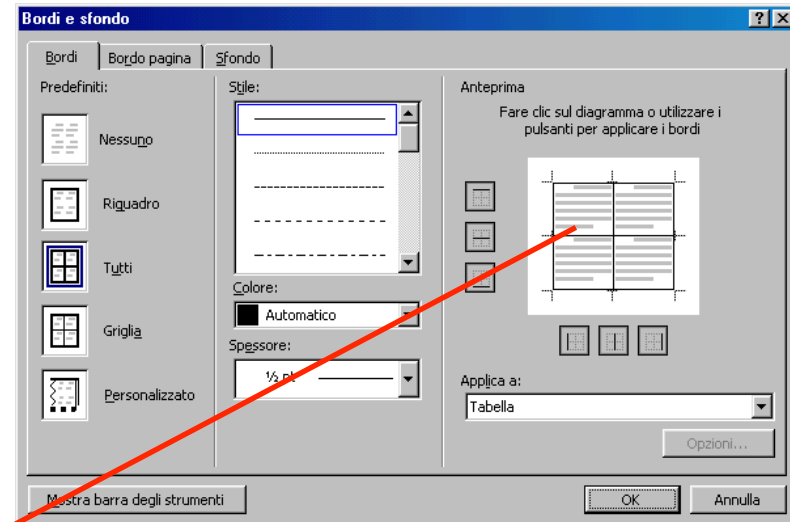
- Taglia
- Copia
- Incolla
- Inserisci celle...
- Elimina celle...
- Unisci celle**
- Disegna tabella
- Bordi e sfondo...
- Orientamento testo...
- Allineamento

Menu Options (Right):

- Taglia
- Copia
- Incolla
- Inserisci righe
- Elimina celle...
- Dividi celle...**
- Disegna tabella
- Bordi e sfondo...
- Formattazione automatica tabella...
- Orientamento testo...
- Allineamento
- Elenchi puntati e numerati...

Inserimento di tabelle/4

- La funzionalità **Bordi e sfondo** permette di personalizzare bordi e sfondo delle celle.



Griglia di controllo

- La voce **Mostra/Nascondi Griglia** controlla la visualizzazione della griglia di controllo della tabella.

Intestazione e pié di pagina/1

- La funzionalità **Bordi e sfondo** permette di personalizzare bordi e sfondo delle celle.